UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/575,650	03/05/2007	Peter Bennett	851963.424USPC	2255

38106 7590 09/26/2011

SEED INTELLECTUAL PROPERTY LAW GROUP PLLC
701 FIFTH AVENUE, SUITE 5400
SEATTLE, WA 98104-7092

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
09/26/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/575,650	BENNETT ET AL.	
	Examiner	Art Unit	
	KAVEH ABRISHAMKAR	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 April 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-18 and 24-29* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-18 and 24-29* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/19/2011*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on April 30, 2010 has been entered.

1. Claims 1-18, and 24-29 are currently pending consideration.

Information Disclosure Statement

2. The initialed and dated copy of the Applicant's Information Disclosure Statement (IDS), received on 7/19/2011, is attached to this Office Action.

Response to Arguments

Applicant's arguments filed on April 30, 2010 have been fully considered but they are not persuasive for the following reasons:

The Applicant argues that the Cited Prior Art (CPA), Bowman (U.S. Patent 5,999,623), does not teach storing a key without requiring the reception of a transmitted key. This argument is not found persuasive. Applicant argues that Bowman requires the reception of an S-key value which is provided to the receiver station before

generating the decryption key. The Examiner contends that this is only in an alternate embodiment (Bowman: column 7, lines 40-55: see "in other embodiments"). However, the Examiner refers to the portion of Bowman which states that the memory stores predefined algorithm, namely the Key-Generator (KG) algorithm , which generates a D-key to be used by the Decryption Processing Block (DPB) for decrypting the encrypted information (column 7, lines 29-39). This key generation and storing all takes place on the smart card (Bowman: Figure 6), and therefore, the D-key which is used to decrypt the encrypted information is stored as it is used to decrypt the encrypted information which is received (column 7, lines 34-38). Therefore, the arguments are not found persuasive, and the rejection is maintained as given below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-18, and 24-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bowman et al. (U.S. Patent 5,999,623) in view of Johnson (U.S. Patent 7,143,294).

Regarding claim 1, Bowman discloses:

A semiconductor integrated circuit for use in an audio-video device arranged to produce audio-video signals, comprising:

an input interface for receipt of a received encrypted enable signal (column 2, lines 26-30: *authorized receiver receives an encrypted signal*);

an output interface for output of audio-video signals (Fig. 4b: step AJ: *outputs decrypted information*);

one or more hardware circuit portions each arranged to process data in relation to the audio-video signals (column 7, lines 5-17: *receives encrypted transmission and decrypts the transmission*);

a first decryption circuit arranged to receive the encrypted enable signal and to decrypt the encrypted enable signal in accordance with a key stored on the integrated circuit to provide a plain text message and without requiring receipt of one or more transmitted keys (column 7, lines 5-17: *receives encrypted transmission and decrypts the transmission;* column 7, lines 29-39: *wherein the key is generated and stored all on the smart card*);

a store containing a stored value for the circuit (column 7, lines 18-27: *the memory stores at least two pre-defined constants used to derive the decryption key*);

a second decryption circuit in one or more hardware circuit portions and arranged to receive a common key from a common key store in the integrated circuit and to decrypt the received encrypted broadcast signal in response to receipt of the common

key and the generation of the enable signal (column 6, lines 40-55*: wherein the s-key values is provided to a receiver from a data table*).

Bowman does not explicitly teach an enabling circuit to selectively restrict, deny or allow operation of a hardware circuit portion and a comparison circuit to compare the plain text message to the stored value to instruct the enabling device. Johnson, in an analogous art, discloses comparing a stored key against a received decrypted key, and if they match, the comparator sends an enable signal to a multiplexer (Johnson: column 6, lines 10-20). It would have been obvious to one of ordinary skill in the art to implement the enabling circuit of Johnson into the system of Bowman in order to secure the system from attack by an unauthorized party (Johnson: column 3, lines 50-55).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 1 wherein the enabling circuit comprises one or more switch elements arranged to selectively interrupt a data pathway to, from, or within at least one of the one or more of the hardware circuit portions (Johnson: column 6, lines 10-20: *enabling circuit*).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 2 wherein the data pathway is a critical data pathway, whereby interruption of the pathway prevents

operation of the at least one of the one or more hardware circuit portions (Johnson: column 6, lines 10-42).

Claim 4 is rejected as applied above in rejecting claim 2. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 2 wherein the data pathway relates to a clock of one or more hardware circuit portions, whereby interruption of the data pathway causes the clock to run slower than normal (Johnson: column 6, lines 10-42).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 4 wherein the one of the one or more hardware circuit portions is a main CPU of the semiconductor integrated circuit (column 6, lines 10-42).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Bowman discloses:

The semiconductor integrated circuit according to claim 2 wherein the at least one of the one or more hardware circuit portions is a display engine, whereby interruption of the data pathway causes the video signals at the output interface to be interrupted or impaired (Fig. 4b: step AJ: *outputs decrypted information*).

Claim 7 is rejected as applied above in rejecting claim 2. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 2 wherein the at least one of the one or more hardware circuit portions is a data port of the semiconductor integrated circuit, whereby interruption of the data pathway prevents operation of the data port (column 6, lines 10-42).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Bowman discloses:

The semiconductor integrated circuit according to claim 1 wherein the input interface is arranged to receive the encrypted enable signal from a broadcast signal (Fig. 4b: step AJ: *outputs decrypted information*).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Bowman discloses:

The semiconductor integrated circuit according to claim 1 wherein the input interface is arranged to receive the encrypted enable signal from a manual input device (Fig. 4b: step AJ: *outputs decrypted information*).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 1 wherein the input interface is arranged to receive the encrypted enable signal from another device (column 6, lines 10-42: *signal received from the comparator device*).

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 1 wherein the enabling circuit comprises a store arranged to store indications of hardware circuit elements to be restricted, denied, or allowed to operate (column 6, lines 10-42).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 11 wherein the store comprises one or more hardware fuses (column 6, lines 10-42).

Claim 13 is rejected as applied above in rejecting claim 11. Furthermore, Bowman discloses:

The semiconductor integrated circuit according to claim 11 wherein the store comprises a non-volatile memory (column 7, lines 18-27: *the memory stores at least two pre-defined constants used to derive the decryption key*).

Claim 14 is rejected as applied above in rejecting claim 1. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 1 wherein the enabling circuit is arranged to extract from the plain text message indications of which hardware circuit elements should be restricted, denied, or allowed to operate (column 6, lines 10-42).

Claim 15 is rejected as applied above in rejecting claim 1. Furthermore, Bowman discloses:

The semiconductor integrated circuit according to claim 1 wherein the semiconductor integrated circuit is a monolithic circuit for decryption of broadcast audio-video signals (column 7, lines 5-14: *a smart card for decrypting video transmissions*).

Claim 16 is rejected as applied above in rejecting claim 2. Furthermore, Bowman discloses:

The semiconductor integrated circuit according to claim 2 wherein the at least one of the one or more hardware circuit portions relates to storing audio-video signals to an external storage device, whereby the enabling circuit is arranged to selectively restrict, deny, or allow storage of the audio-video signals produced by the circuit (column 7, lines 5-27).

Claim 17 is rejected as applied above in rejecting claim 2. Furthermore, Bowman teaches:

The semiconductor integrated circuit according to claim 2 comprising an input for receiving broadcast signals from a broadcast network from which the audio-video signals are produced, and wherein the at least one of the one or more hardware circuit portions relates to production of the audio-video signals (column 7, lines 5-14: *a smart card for decrypting video transmissions*).

However, Bowman does not explicitly state that the enabling circuit is arranged to selectively, restrict, deny, or allow the production of the audio-video signals. Johnson, in an analogous art, discloses comparing a stored key against a received decrypted key, and if they match, the comparator sends an enable signal to a multiplexer (Johnson: column 6, lines 10-20). It would have been obvious to one of ordinary skill in the art to implement the enabling circuit of Johnson into the system of Bowman in order to secure the system from attack by an unauthorized party (Johnson: column 3, lines 50-55).

Regarding claim 18, Bowman discloses:

A television decoder comprising:

a semiconductor integrated circuit that comprises an input interface for receipt of a received encrypted enable signal (column 2, lines 26-30: *authorized receiver receives an encrypted signal*);

an output interface for output of audio-video signals (Fig. 4b: step AJ: *outputs decrypted information*);

one or more hardware circuit portions each arranged to process data in relation to the audio-video signals (column 7, lines 5-17: *receives encrypted transmission and decrypts the transmission*):

a first decryption circuit arranged to receive the encrypted enable signal and to decrypt the encrypted enable signal in accordance with a key stored on the integrated circuit prior to reception of the encrypted broadcast signals and to provide a plain text message without requiring receipt of one or more transmitted keys (column 7, lines 5-17: *receives encrypted transmission and decrypts the transmission;* column 7, lines 29-39: *wherein the key is generated and stored all on the smart card*);

a store containing a stored value for the circuit (column 7, lines 18-27: *the memory stores at least two pre-defined constants used to derive the decryption key*).

a second decryption circuit in one or more hardware circuit portions and arranged to receive a common key from a common key store in the integrated circuit and to decrypt the received encrypted broadcast signal in response to receipt of the common key and the generation of the enable signal (column 6, lines 40-55*: wherein the s-key values is provided to a receiver from a data table*).

Bowman does not explicitly teach an enabling circuit to selectively restrict, deny or allow operation of a hardware circuit portion and a comparison circuit to compare the plain text message to the stored value to instruct the enabling device. Johnson, in an analogous art, discloses comparing a stored key against a received decrypted key, and

if they match, the comparator sends an enable signal to a multiplexer (Johnson: column 6, lines 10-20). It would have been obvious to one of ordinary skill in the art to implement the enabling circuit of Johnson into the system of Bowman in order to secure the system from attack by an unauthorized party (Johnson: column 3, lines 50-55).

Regarding claim 24, Bowman discloses:

A circuit, comprising:

a first decryption circuit adapted to decrypt an encrypted enable signal in accordance with a pre-stored key that is stored in the first decryption circuit and to output a plain text message without requiring receipt of one or more transmitted keys (column 7, lines 5-17: *receives encrypted transmission and decrypts the transmission;* column 7, lines 29-39: *wherein the key is generated and stored all on the smart card*);

a second decryption circuit adapted to decrypt the encrypted broadcast signals and produce the audio-video signals in response to receipt of a pre-stored common key and the control signal (column 6, lines 40-55*: wherein the s-key values is provided to a receiver from a data table*).

Bowman does not explicitly disclose a comparison circuit adapted to compare the plain text message with a stored value and selectively output a control signal if the plain text message matches the stored value. Johnson, in an analogous art, discloses comparing a stored key against a received decrypted key, and if they match, the comparator sends an enable signal to a multiplexer (Johnson: column 6, lines 10-20). It would have been obvious to one of ordinary skill in the art to implement the enabling

circuit of Johnson into the system of Bowman in order to secure the system from attack by an unauthorized party (Johnson: column 3, lines 50-55).

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Johnson discloses:

The circuit of claim 24, comprising an enabling circuit adapted to selectively enable, disable, and restrict operation of at least one other circuit in response to the control signal (column 6, lines 10-42).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Johnson discloses:

The circuit of claim 25, wherein the enable circuit is adapted to select which of a plurality of other circuits to selectively enable, disable, and restrict operation in response to the control signal (column 6, lines 10-42).

Regarding claim 27, Bowman discloses:

A method of controlling a circuit for receiving encrypted broadcast signals and producing audio-video signals therefrom, comprising:

decrypting an encrypted enable signal in accordance with a pre-stored key without requiring receipt of one or more transmitted keys and to output a plain text message (column 7, lines 5-17: *receives encrypted transmission and decrypts the*

transmission; column 7, lines 29-39: *wherein the key is generated and stored all on the smart card*);

decrypting the encrypted broadcast signals and produce the audio-video signals in response to receipt of a pre-stored common key and the control signal (column 6, lines 40-55*: wherein the s-key values is provided to a receiver from a data table*).

Bowman does not explicitly disclose comparing the plain text message with a stored value and selectively outputting a control signal if the plain text message matches the stored value. Johnson, in an analogous art, discloses comparing a stored key against a received decrypted key, and if they match, the comparator sends an enable signal to a multiplexer (Johnson: column 6, lines 10-20). It would have been obvious to one of ordinary skill in the art to implement the enabling circuit of Johnson into the system of Bowman in order to secure the system from attack by an unauthorized party (Johnson: column 3, lines 50-55).

Claim 28 is rejected as applied above in rejecting claim 27. Furthermore, Johnson discloses:

The method of claim 27, comprising the further step of selectively enabling, disabling, and restricting operation of at least one other circuit in response to the control signal (column 6, lines 10-42).

Claim 29 is rejected as applied above in rejecting claim 28. Furthermore, Johnson discloses:

The method of claim 28, wherein selectively enabling, disabling, and restricting operation comprises selecting which of a plurality of other circuits to selectively enable, disable, and restrict operation in response to the control signal (column 6, lines 10-42).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/

Primary Examiner, Art Unit 2431

/K. A./
09/13/2011
Primary Examiner, Art Unit 2431